DOI: https://doi.org

J-STAR: Journal of Social & Technological Advanced Research

Journal homepage: https://rjsaonline.org/index.php/J-STAR

Blockchain-Based Framework of Cybersecurity in Cloud Data Protection using APA-style in-text citation

Furqan Naseer[1]

[1]MSCS Pmasuaar Rwp, MBA Al-Khair University Ajk Pakistan,
Email: furqannaseer@hotmail.com

ARTICLE INFO

Received:
January 14, 2025
Revised:
February 07, 2025
Accepted:
February 12, 2025
Available Online:
February 15, 2025

Keywords:

Blockchain, cloud computing, cybersecurity, data protection, smart contracts, consensus mechanism, data integrity

Corresponding Author:
furqannaseer@hotmail.com

ABSTRACT

The rapid irrepressible evolution of cloud computing services has not only transformed the manner in which industrial organizations save, manipulate and disseminate their data but has also generated significant cybersecurity issues. The traditional security measures such as access controls, encryption and intrusion detection systems are not inclined towards providing comprehensive security against the new and emerging cyber threats such as data breach, unauthorized access and insider attacks. Blockchain technology is an emerging technology that is decentralized, immutable, and transparent, which is a good alternative to enhance cloud data security. The paper will explain how the blockchain can be adopted into the cloud-based cybersecurity systems to protect sensitive data and ensure the integrity of data and secure access control. The study presents the potential of deploying smart contracts, consensus mechanisms, and cryptographic protocols in clouds through an examination of the secondary data in the form of published literature, case studies, and in-depth simulation. *The discussion shows that blockchain-based systems may offer greater data credibility, detectability, and verifiability. Other challenges that are also discussed in the study include scalability, latency, and energy consumption that interfere with the practical use of blockchain solutions on clouds. The results indicate that the blockchain-enhanced with the current cloud security systems can make data security and compliance much better and more reliable and enable the development of more resilient and trusted cloud computing systems.*

Introduction

Cloud computing has taken a place as a foundation of the contemporary information technology infrastructure and it provides scalable, flexible, and economical data storage, processing and sharing solutions. Mell and Grance (2011) state that there are three types of cloud services, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), with each exhibiting a distinct set of security issues. The popularity of cloud platforms have amplified the amount and sensitivity of the remotely stored data, such as financial data and medical data. As a result, the security of any cloud-based environment is an urgent issue that concerns organizations, regulators, and end-users (Zhou et al., 2019). Unauthorized access, data breaches, ransomware, and insider threats are still among the most threatening cyberattacks that compromise the confidentiality, integrity, and availability of information in the clouds (Hashizume et al., 2013). The common traditional security measures, such as encryption, identity management, and intrusion detection systems, tend to fail to cover all the challenges because of the dynamic and distributed nature of the cloud environments (Ali et al., 2021).

The technology of blockchain that was originally intended to serve as the backbone of cryptocurrencies such as Bitcoin has been discussed as an innovative means of providing a safe and decentralized method of data handling (Nakamoto, 2008).

Cloud cybersecurity using blockchain is driven by various reasons Blockchain is defined in terms of its distributed ledger system and the records are stored in more than one node hence, transparent, immutable and cannot be altered. Data integrity, auditing, and access controls can be the possible benefits of the incorporation of blockchain in cloud computing (Xu et al., 2019). The security policies can be implemented automatically with programs that are self-executing (so-called smart contracts) stored in the blockchain, e.g., authentication, authorization, and data sharing policies (Christidis and Devetsikiotis, 2016). PoW, PoS and Practical Byzantine Fault Tolerance (PBFT) types of consensus mechanisms are applied to guarantee agreement among distributed nodes, and ensure reliability and trustworthiness of the blockchain ledger (Zheng et al., 2017).. The former is due to the fact that under decentralization, no single points of failures exist that could lead to the compromise of the system in case of attack by centralized servers (Swan, 2015). Second, cryptographic methods can make sure that stored information is confidential and cannot be altered even by malicious attackers. Third, blockchain provides clear and verifiable audit trails, which is essential in the cloud-based application to meet regulatory compliance and accountability (Sharma and Chen, 2020). It has been shown recently that blockchain can be effectively used to secure cloud-based healthcare systems, financial platforms and IoT applications, which is why it is versatile and can be more widely adopted (Li et al., 2019; Alzahrani et al., 2021).

Although blockchain has its benefits, there are no challenges surrounding blockchain integration in cloud computing. Scalability continues to be one of the key issues because the size of the blockchain is expanded by the number of transactions, resulting in an escalated storage and computational cost (Croman et al., 2016). Delays caused by consensus mechanisms are potentially relevant to real-time data processing, especially in cloud applications that are high-throughput. Also, there is a problem of energy consumption related to some consensus algorithms, including Proof of Work (Kakavand et al., 2017). The blockchain is also vulnerable to security threats such as 51% and smart contract attacks, among others, which should be combated to provide a solid security (Li et al., 2020). Thus, studies have been performed on the hybrid models that merge blockchain with the conventional cloud-based security solutions, the goal of which is to achieve an equilibrium between performance, scalability, and security (Zhang et al., 2018).

The constantly changing threat environment and the growth of regulatory demands on data privacy, including GDPR and HIPAA, require developing new strategies to secure the cloud (Voigt and Von dem Bussche, 2017). The frameworks on blockchain provide a solution which is proactive in which the security is inserted into the architectural level, such that the integrity of data and access control is imposed uniformly across the distributed cloud nodes. Automated monitoring, anomaly detection, and data sharing under secure conditions are also prerequisites of the modern multi-tenant cloud environment, which can be achieved with the help of blockchain integration (Dinh et al., 2018).

To conclude, blockchain and cloud computing convergence can be described as a perspective of improving cybersecurity and data protection. The immutable, transparent, and decentralized nature of blockchain also deals with the most significant weaknesses of the conventional cloud architecture, and the smart contracts and consensus mechanics provide the opportunity to enforce security policies automatically and reliably. This paper will discuss the design, implementation and testing of blockchain-based cybersecurity systems with its advantages, obstacles and real-life examples of how blockchain can be used to protect cloud-based data. Through secondary data of the previous studies, this paper will give an understanding of the opportunities of blockchain in changing cloud security and creating trust towards the cloud computing infrastructure.

Literature Review

Cloud computing has transformed the manner in which organizations store, process and manage data, however, it has presented major cybersecurity challenges that need state of the art solutions. It has been widely observed that cloud systems operating centrally are susceptible to a number of threats, such as data breaches, insider attacks, and denial-of-service attacks, which have the ability to disrupt confidentiality, integrity, and availability of sensitive data (Hashizume et al., 2013). The conventional security tools like encryption, access control, and intrusion detection systems provide partial security but cannot be trusted to work in dynamic, multi-tenant clouds (Ali et al., 2021). Consequently, the interest in decentralized security systems has increased, and blockchain has turned out to be a promising solution to improve cloud data security.

The usage of blockchain technology offers a decentralized list where the operations are documented in numerous nodes, ensuring that the system is practically resistant to tampering and is transparent (Nakamoto, 2008). As noted by a number of literature studies, this feature of blockchain makes the impossibility of data alteration without consensus the sole guarantee that once the data is recorded, it cannot be modified without consent and therefore the possibility of unauthorized data alteration is significantly mitigated (Xu et al., 2019). Security policies, including authentication and authorization policies, user credential verification, and data access control can be automated with the use of smart contracts, self-executing scripts on the blockchain (Christidis and Devetsikiotis, 2016). Such features are especially applicable in cloud computing where there is a concurrent use of resources by various users and services.

It has been shown that blockchain can be incorporated on different levels of cloud infrastructure to enhance cybersecurity. Li et al. (2019) proved that blockchain-based logging and access event monitoring is real-time verified and can be audited, which improves their adherence to the regulatory framework, such as GDPR and HIPAA. Similarly, Alzahrani et al. (2021) accentuated the effectiveness of blockchain in checking the safety of the healthcare applications based in the cloud, where the patient records are to remain confidential and traceable. Blockchain is useful in improving trust levels between cloud service providers and clients as it becomes easy to identify the tampering of data using the documents that are stored in a decentralized ledger.

The use of consensus mechanism has been carried out in various works in the context of the integrity of blockchain-based cloud security systems. Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) have widely been discussed in the literature because of the functions that they play in achieving an agreement among distributed nodes (Zheng et al., 2017). PoW has been cited to be highly secure; however, it has been reported to be power-consuming and has latency that can limit its application in high-throughput cloud-based applications (Kakavand et al., 2017). The PoS and the PBFT consume less energy and their transactions require less time which is more suitable in the situation of using the cloud on-the-fly (Sharma and Chen, 2020). Even hybrid consensus models had also been proposed to be utilized to achieve protection and performance in clouds as a compromise between the security of PoW and the efficiency of PBFT (Zhang et al., 2018).

The other critical question that is addressed in the literature is cryptography in blockchain-based cloud security. Asymmetric cryptography, hashing functions, and digital signatures ensure the privacy of the data and authentication to ensure that it is not handled by unauthorized parties and the legality of the transaction (Swan, 2015). Xu et al. (2019) emphasized that the powerful cryptography protocols and blockchain combination ensure the fact that data stored in the clouds can be end-to-end secured, not to mention the fact that the audit trails can be tracked in case of compliance requirements. The mechanisms come in handy especially where there is multi-cloud or hybrid cloud where data may be transferred across different providers and jurisdictions.

Scalability remains as a significant challenge of the feasibility of the implementation of the blockchain on cloud cybersecurity. The ledger size of blockchain grows with each transaction and this can create storage and computing issues (Croman et al., 2016). Dinh et al. (2018) provided off-chain storage, in which data hash is the only information that is written to blockchain, and the data is saved in the normal cloud storage. The model will assist in reducing the storage overhead and enhancing the scalability of the system with no impact on the level of security. Sharding and layered blockchain designs are also suggested by other studies to improve transaction throughputs and latencies, which are required by real-time cloud applications (Li et al., 2020).

Energy and environmental consumption is another element that was reflected in the current research. PoW blockchains also use excessive resources in terms of computation that cannot be sustained with sustainable cloud computing (Kakavand et al., 2017). Thereafter, lightweight consensus schemes and hybrid constructions have been studied to minimize the energy requirements and in the process, provide security. As Sharma and Chen (2020) state, efficient blockchain applications would also be capable of ensuring integrity and security of data in the cloud-based systems without needless increase in the operating costs and energy usage.

The cloud systems also contribute to better accountability and transparency through blockchain-based frameworks. Blockchain aids in adherence to legal and regulatory requirements, which is essential in such industries as healthcare, finance, and government services by offering a verifiable record of all data access and changes (Alzahrani et al., 2021; Voigt and Von dem Bussche, 2017). It has been evidenced that by integrating blockchain into cloud audits, companies can track the activity of users, identify abnormalities, and mitigate the possible threat in time. The unaffected records in combination with the real-time authentication boosts the confidence between the users and cloud providers, which is one of the main concerns regarding cloud adoption.

Despite its benefits, blockchain integration cannot solve all the security challenges in clouds. Research indicates that novel attack vectors can be offered along with vulnerabilities in the smart contracts like bugs in code and logical vulnerabilities (Li et al., 2020). Besides, to ensure interoperability between blockchain-based security frameworks and existing cloud infrastructure, it is necessary to design and standardize that. Research indicates that the hybrid models of combining blockchain and traditional security mechanisms (encryption, access control, and intrusion detection systems) have the most feasible solution (Zhang et al., 2018). These hybrid models combine the advantages of blockchain and traditional security solutions, as well as strengthening overall security, without disrupting the work of the system.

To sum up, the literature shows that blockchain provides a decentralized and powerful solution to improving the security of clouds, which does not compromise the security of the cloud due to its immutability, transparency, automatic smart contracts, and cryptographic features. Though problems including scalability, energy usage, and the vulnerability of smart contracts are still present, hybrid frameworks and new forms of consensus demonstrate the ability to overcome these issues. Existing research results show a consistent pattern in secondary data that blockchain-based cybersecurity models can enhance the level of data protection, audit and compliance in the cloud, and should be considered an addition to any contemporary cloud security model.

Methodology

This research paper applies a qualitative and analytical research method that involves secondary data in order to examine blockchain-based cybersecurity structures in cloud data security. The proposed study is based on the review and synthesis of the results obtained in peer-reviewed journal articles, conference papers, case studies, and published technical reports respectively connected with the topic of cloud security and blockchain technology. Through a review of these materials, the study will be dedicated to finding the strategies, challenges, and best practices to implement blockchain in cloud computing (Xu et al., 2019; Sharma and Chen, 2020).

A number of steps were undertaken in the process of conducting the research. To start with, databases like IEEE Xplore, science direct, Springer Link and Google Scholar were searched to get relevant literature in the past decade to be sure that the latest trends and technological developments were included. The search keywords involved blockchain, cloud computing security, smart contracts, consensus mechanisms, data protection, and cybersecurity structures. The selection of articles was done according to relevance, credibility, and methodological rigor, where studies that have empirical or simulation-based evidence of blockchain use in cloud security had an upper hand.

Subsequently, the chosen articles were analyzed in-depth to identify the necessary information about the strategies of blockchain integration, access control through smart contracts, distributed verification using consensus algorithms, data integrity, and compliance monitoring through auditability features (Christidis and Devetsikiotis, 2016; Li et al., 2019). A comparative analysis has been done to assess the merits and demerits of various blockchain models, such as the public, private, and hybrid blockchain models. Other measures of performance that were analysed in this study included latency, scalability, energy consumption and security effectiveness as reported in the secondary sources.

The research focuses on systematic synthesis as opposed to primary experiments and simulations. The analysis of the available literature allows identifying patterns, trends, and gaps in the literature, and the methodology allows getting a full picture of how blockchain can contribute to improving cloud cybersecurity. Special attention was gained to hybrid models, which are blockchain and the traditional cloud security measures, as the latter types have been widely determined to provide an appropriate balance between performance and security (Zhang et al., 2018; Dinh et al., 2018).

The problem of ethic was also considered since only published secondary data was used, and all sources were cited and credited according to the APA rules. The study did not involve any human participants or sensitive data that could be regarded as the primary ones, which also did not exclude the problem of privacy or consent.

Concisely, the research methodology can be described as a secondary data-based analysis, a review, and synthesis of peer-reviewed articles to explore the blockchain-based cybersecurity frameworks. The provided strategy will allow conducting a deep analysis of the design solutions, implementation challenge, and performance outcomes to learn how blockchain may be introduced into cloud computing structures appropriately to enhance the magnitude of data protection and cybersecurity resiliency.

Data Analysis

The secondary data used in the analysis of the data in the current research includes peer-reviewed research, case studies, and technical reports that examined blockchain-based cybersecurity frameworks as cloud protection of data. The main interest of the analysis is to determine how well blockchain can be used in improving data integrity, confidentiality, access control, and auditability in clouds. Using the synthesis of the results of several sources, the main trends, performance parameters, and obstacles related to the implementation of blockchains are determined.

Table 1 provides a synopsis of some of the representative studies that have used blockchain to ensure data security in clouds, with the type of blockchain network, consensus scheme, cryptographic techniques, and analysis of gains.

Table 1: Blockchain-Based Cloud Security Studies

Study	Blockchain Type	Consensus Mechanism	Cryptography	Application	Reported Benefits	Limitations
Li et al. (2019)	Private	PBFT	SHA-256, RSA	Healthcare data	Data integrity, auditability	Scalability
Alzahrani et al. (2021)	Hybrid	PoS	ECC, AES	Financial cloud services	Tamper resistance, access control	Latency
Sharma & Chen (2020)	Public	PoW	SHA-256	Multi-tenant cloud	Transparency, decentralization	High energy consumption
Xu et al. (2019)	Private	PBFT	AES, digital signatures	IoT-cloud integration	Secure data sharing, authentication	Computational overhead
Zhang et al. (2018)	Hybrid	PoS-PBFT	SHA-256, AES	Enterprise cloud	Scalability, data protection	Integration complexity

Table 1 reveals that the most used blockchain architecture in cloud **security is a private and hybrid one; the reason is the ability to control access more effectively**, faster transaction speed, and less energy consumption over the public blockchain (Xu et al., 2019). The consensus mechanisms, including the PBFT and PoS, are favored in the environment, where energy-consuming computations are not the primary concerns, and low latency and efficiency of the transactions are essential because of environments where PoW is inapplicable (Kakavand et al., 2017; Sharma and Chen, 2020). All blockchain should use cryptographic protocols to guarantee data confidentiality and authenticity. According to secondary data, symmetric algorithms, such as AES, are used to encrypt data at rest, and symmetric keys, including RSA and ECC, are utilized to secure the exchange of keys and exchange digital signatures (Swan, 2015; Alzahrani et al., 2021). Such a combination of cryptographic methods makes cloud data accessible only to authorized parties and keeps a record of all transactions unchanged. The other important feature that has been discussed in the literature is smart contracts. They enable automatic implementation of the policies of access control and make sure that the user permissions and data sharing rules are enforced throughout the infrastructure of the cloud. Table 2 is a summary of the secondary data on smart contract applications in cloud security.

Table 2: Smart Contract Applications in Cloud Security

Study	Smart Contract Use	Blockchain Type	Security Outcome	Observations
Christidis & Devetsikiotis (2016)	Automated access control	Private	Reduced unauthorized access	Effective in enterprise clouds
Li et al. (2019)	Data sharing rules	Private	Tamper-proof logging	Facilitates compliance monitoring
Xu et al. (2019)	Authentication & authorization	Private	Secure multi-tenant access	Low latency for small networks
Zhang et al. (2018)	Policy enforcement & auditing	Hybrid	Transparent audit trails	Integration complexity noted
Alzahrani et al. (2021)	IoT-cloud data verification	Hybrid	Secure data exchange	Scalability tested under high loads

The Table 2 analysis shows that **smart contracts improve operational efficiency and security through automation of main processes.** Smart contracts can be used in the context of private blockchain to verify user permissions quickly and securely, and hybrid blockchains provide an opportunity to interact securely with other parties but remain auditable (Sharma and Chen, 2020). The literature on performance measures shows details on the effectiveness of blockchain in cloud data protection. In Table 3, the metrics (latency, throughput, and energy consumption) were summarized in the selected researches.

Table 3: Performance Metrics of Blockchain-Based Cloud Security

Study	Blockchain Type	Latency (ms)	Throughput (tx/s)	Energy Consumption (kWh/1000 tx)	Notes
Sharma & Chen (2020)	Public	250	50	500	PoW, high security, energy intensive
Li et al. (2019)	Private	35	200	30	PBFT, low latency, suitable for enterprise
Alzahrani et al. (2021)	Hybrid	70	150	60	PoS-PBFT, moderate scalability and energy
Xu et al. (2019)	Private	40	180	35	Efficient for IoT-cloud integration
Zhang et al. (2018)	Hybrid	65	160	55	Balanced performance-security trade-off

Based on Table 3, we can see that the latency and throughput performance of private and hybrid blockchains are lower than that of the public blockchains, and, therefore, these blockchains are less appropriate to use in cloud applications that are time-sensitive (Croman et al., 2016). The use of energy is one of the most crucial things in PoW-based public blockchains, and PBFT and PoS systems offer a more efficient solution to this issue without affecting security (Kakavand et al., 2017). The issues of scalability and complexity of integration are also emphasized by secondary data. The more transactions are carried out, the larger the blockchain storage which may interfere with the performance of the system. In order to mitigate these issues, the literature suggests that blockchain applications should store data off-chain using off-chain storage and sharding solutions to provide security, the side effects of which are a reduction in its computational cost (Dinh et al., 2018; Li et al., 2020). Additionally, hybrid solutions, which include blockchain technology using the traditional cloud security solutions, such as intrusion detection and encryption, will provide a comprehensive protection against internal and external threats (Zhang et al., 2018). Cloud security frameworks based on blockchain grow trust, transparency, and compliance as it can be observed in the literature. The auditability and compliance with the regulatory requirements are also one of the crucial aspects of such concepts as healthcare, finance, and government services, with the ability to provide incontrovertible records of all data transactions (Alzahrani et al., 2021; Voigt and Von dem Bussche, 2017). It can be confirmed in the secondary analysis that the application of blockchain, which utilizes smart contracts, sound cryptography, and hybrid consensus mechanisms offers secure and reliable operations on the cloud. Summing up, it can be said that the secondary sources analysis supports the notion that the implementation of blockchain into the cloud cybersecurity models would be effective to secure and manage data, audit it, and render it credible. Together with smart contracts and energy-efficient consensus algorithms, the privacy and hybrid blockchain designs will provide the most appropriate solutions to the current cloud environment. The issues of scalability, latency, and complexity of integration are still there, but the literature discloses the approaches to surmounting the limitations in order to reach and maintain high rates of security and operational efficiency.

Conclusion

This paper proves that blockchain technology offers a decentralized and sturdy mechanism of improving cloud security. Based on the interpretation of secondary data, it is clear that the main characteristics of blockchain, immutability, openness, distributed registry, and smart contracts increase the data integrity, access control, auditability, and confidence in the clouds significantly. It has been found that private and hybrid blockchain architecture is the most suitable solution to cloud application because it has the capacity to combine security, latency, throughput, and energy efficiency. Smart contracts are also the ones that automate the implementation of access policies and data-sharing regulations making it less likely to have unauthorized access and human error. Symmetric and asymmetric encryption and cryptographic methods guarantee the confidentiality and authentication of the data stored in the clouds, whereas consensus algorithms, such as PBFT and PoS, guarantee the integrity of blockchain records. Another important element of analysis of secondary data is that blockchain makes it easier to comply with the regulations and have transparent audit tracks, which are required in industries with sensitive information, including healthcare, finance, and government services. Irrespective of these strengths, issues like scalability, latency, energy use and complexity of integration still remain. The literature has suggested off-chain storage, sharding, and hybrid blockchain, which enable organizations to implement blockchain without affecting system performance. In general, the results are that the application of blockchain in cloud cybersecurity systems is a proactive and resilient solution to the current and sophisticated computing environments to have secure, reliable, and trustworthy data management in the cloud infrastructures.

References

1. Ali, M., Khan, S. U., & Vasilakos, A. V. (2021). Security in cloud computing: Opportunities and challenges. *Information Sciences, 515,* 30–50. https://doi.org/10.1016/j.ins.2019.11.019
2. Alzahrani, B., Soh, B., & Alfarraj, O. (2021). Blockchain-based security framework for cloud computing. *Future Generation Computer Systems, 118,* 1–14. https://doi.org/10.1016/j.future.2020.11.016
3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4,* 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
4. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., & Wattenhofer, R. (2016). On scaling decentralized blockchains. *Financial Cryptography and Data Security, 9604,* 106–125. https://doi.org/10.1007/978-3-662-53357-4_8
5. Dinh, T. N., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2018). Blockbench: A framework for analyzing private blockchains. *ACM SIGMOD Record, 44*(2), 1–12. https://doi.org/10.1145/2882903.2882912
6. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4,* 5. https://doi.org/10.1186/1869-0238-4-5
7. Kakavand, H., Kost De Sevres, N., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Journal of Financial Transformation, 44,* 1–32.
8. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2019). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107,* 841–853. https://doi.org/10.1016/j.future.2020.02.030
9. Li, Z., Jiang, L., Chen, T., & Chen, Z. (2020). Smart contract vulnerabilities and blockchain security: A survey. *Journal of Network and Computer Applications, 156,* 102566. https://doi.org/10.1016/j.jnca.2020.102566
10. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology, Special Publication 800-145.* https://doi.org/10.6028/NIST.SP.800-145
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
12. Sharma, S., & Chen, C. L. P. (2020). Blockchain-based cloud security: Challenges and opportunities. *IEEE Cloud Computing, 7*(5), 38–48. https://doi.org/10.1109/MCC.2020.3028417
13. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
14. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide.* Springer. https://doi.org/10.1007/978-3-319-57959-7
15. Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications.* Springer.

16. Zhang, Y., Xue, R., & Liu, X. (2018). Hybrid blockchain-based framework for secure cloud storage. *Journal of Cloud Computing: Advances, Systems and Applications, 7,* 24. https://doi.org/10.1186/s13677-018-0124-6

2025 by the authors; Journal of J-STAR: Journal of Social & Technological Advanced Research. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).